IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MISSOURI
EASTERN DIVISION

ALAN PRESSWOOD, D.C., P.C., individually and on behalf of all other similarly-situated persons, Plaintiff, v. AMERICAN HOMEPATIENT, INC., a Florida corporation, and JOHN DOES 1-10, Defendants.	)	Civil Action No.4:17-cv-01977-SNLJ **CLASS ACTION**

PLAINTIFF'S MEMORANDUM IN SUPPORT OF MOTION TO COMPEL AND FOR ENTRY OF A PROTECTIVE ORDER REGARDING ELECTRONIC DISCOVERY

Plaintiff Alan Presswood, D.C., P.C. ("Plaintiff"), submits Plaintiff's Memorandum in Support of Motion to Compel and for Entry of a Protective Order Regarding Electronic Discovery.

Introduction

The is a putative Class Action against Defendant American Homepatient, Inc. ("Defendant" or "American Homepatient") regarding unsolicited fax advertisements it sent to Plaintiff (on August 22, 2013), and to other members of the proposed class (the "Fax" or "Subject Faxes"), in violation of the Telephone Consumer Protection Act of 1991 ("TCPA"), 47 U.S.C. § 227(b)(1)(C). (Doc. 1-1, ¶¶ 2, 10). During the course of discovery in this case and in *Radha Geismann. M.D., P.C. v. American Homepatient, Inc.*, Case No. 4:14-cv-01538-RLW, (hereinafter "*Geismann* case"), an earlier case involving the same fax advertisements, Plaintiff learned that Defendant conducted its fax advertising "in-house," using RightFax Version 10 software ("RightFax"). To date, Defendant has failed to produce a single fax transmission log,

variously claiming that it did not routinely keep such records, that even if such records did exist, they would have been automatically overwritten, and that it has searched for but did not find the requested records.

As discussed *infra* by Plaintiff's expert, Robert Biggerstaff ("Biggerstaff"), RightFax software stores records of all faxes sent, even if users have deleted the faxes from their mailboxes. Further, when a user of RightFax deletes a fax, the fax record is saved and marked as belonging to a deleted fax. Biggerstaff is often able to retrieve the deleted data, namely, the data regarding the fax transmissions at issue here, from the hard drives(s) where the RightFax data is stored. Plaintiff requested from Defendant forensic image(s) of Defendant's "servers," which in this case is a storage area network(s) ("SAN"), as well as the specifications of the SAN system to enable the imaging of its SAN network.[1] The purpose of the forensic imaging would be to allow Biggerstaff to search for the missing fax transmission logs. Plaintiff further provided to Defendant a proposed protective order that set forth procedures that would govern the forensic imaging and search by Biggerstaff.

Not surprisingly, Defendant, whose opposition to class certification (and on the merits) will no doubt be premised in part on the (current) absence of fax transmission logs, refused to produce the images or agree to the proposed protective order. Plaintiff now requests that the Court enter an Order requiring Defendant to provide the specifications of its SAN network, *i.e.*, answer Interrogatory No. 22[2], and enter Plaintiff's proposed Protective Order Regarding Electronic Discovery ("EPO"), attached as Exhibit 1. The proposed EPO requires Defendant to permit the imaging of its SAN network, sets forth the protocols to be followed regarding said

[1] A SAN is just a server dedicated to storage, rather than a server that has both storage and applications; it has hard drives for storage just like any other computer and can be imaged the same way.

[2] Defendant should also be required to disclose the operating system and location of its SAN system.

imaging and subsequent search for relevant materials by Biggerstaff, and sets forth procedures to protect the confidentiality of the requested materials. Defendant should not be permitted to thwart Plaintiff's efforts to obtain evidence of the utmost relevance, the fax transmission logs, and at the same time defend this case based on the absence of those same logs.

Relevant Background

A. Defendant used RightFax to send the fax advertisements at issue; the records of such faxing should still be on Defendant's SAN system.

It is undisputed Defendant used RightFax to transmit the Subject Faxes. Plaintiff has attached as Exhibit 2 the Declaration of its expert, Robert Biggerstaff, March 5, 2018. Biggerstaff has substantial experience in the role that computers play in claims under the TCPA, specifically with regard to analyzing computer records to identify persons to whom facsimiles were sent for purposes of class certification and class notice. (Biggerstaff Decl., ¶ 6, Ex. 2). Biggerstaff also has extensive knowledge of facsimile technology and with various types of fax software platforms, including RightFax 10. (*Id*. ¶¶ 7-9, 12-13).

Attached to Biggerstaff's Declaration as Exhibit A is the RightFax Version 10 Server Administrator's Guide ("RightFax Administrator's Guide"). (*Id.*, ¶ 14). Page 289 of RightFax Administrator's Guide states: "RightFax stores records of all faxes, even if users have deleted the faxes from their mailboxes. When a user deletes a fax the fax record is saved and marked as belonging to a deleted fax." (*Id*., ¶ 15, Ex. A at 289). Based on his experience with databases and fax software, as well as his experience with RightFax in particular, Biggerstaff states it is "very likely the records of all faxes would be contained in the SQL database linked to Defendant's RightFax Server." (*Id*., ¶ 16). In many instances, Biggerstaff has been able to recover data regarding fax transmissions from hard drives used by fax platforms such as RightFax despite the custodians of those systems being unaware that such records were stored in

said systems. (*Id*., ¶ 17). Biggerstaff states that using the forensic examination tools that he regularly employs, he is able to retrieve deleted data from the hard drive(s) where the RightFax data is stored, including the storage media of whatever system houses the SQL data for the RightFax server. (*Id*., ¶ 18).

B. Defendant stores its electronic data in a "storage area network," or SAN.

Defendant used a SAN to store their data, described as "multiple hard drives shared to store data." A SAN is just a server dedicated to storage, rather than a server that has both storage and applications, and that it has hard drives for storage just like any other computer and can be imaged the same way as a workstation. (*See* Pl.'s Dec. 21, 2017, Ltr. at 2, Ex. 7). The storage capacity of a SAN is capable of being determined in multiple ways, including directly by the user interface to the SAN, and from knowing the manufacturer and model number of the components of the SAN and of the hard drives installed. (Biggerstaff Decl., ¶ 11, Ex. 2).

C. Defendant refuses to image its servers (SAN).

Defendant has failed to produce any fax transmission logs that would identify the fax numbers to which the images were transmitted, the date and time of each transmissions, and whether the transmissions were successful. Faced with the absence of production of such highly relevant documents and data, and with the *Geismann* case fresh in its mind, Plaintiff made the following production requests of Defendant on September 29, 2017 (several requests were made in the *Geismann* case, *See* Exhibit 3, Pl.'s First Req. for Prod. July 17, 2015):

> **Request No. 5**: Produce a mirror image of each hard drive, backup server, or any device used to send Exhibit A by facsimile transmission during the Relevant Time Period.
>
> **Request No. 8**. Produce a mirror image of each hard drive, backup server, or any device used to create, edit, modify, store, or use in any way any documents or templates used for facsimile transmissions during the Relevant Time Period of any document that promotes, advertises, announces or solicits any property, good or services of Defendant and which was sent by facsimile transmission during the

> Relevant Time Period.
>
> **Request No. 9**: Produce a mirror image of each hard drive, backup server, or any device used to create, edit, modify, store, or use in any way any documents or templates used to transmit Exhibit A which was sent by facsimile transmission during the Relevant Time Period.

(Pl.'s First Req. for Prod., attached as Exhibit 4, at Nos. 5, 8, 9).

In its responses served November 13, 2017, Defendant offered essentially the same response/objection as to each of these Requests:

> Defendant objects to this Request to Produce on grounds that it erroneously assumes "facsimile transmissions" are at issue. Defendant objects to this Request to Produce on grounds that this request seeks information not relevant to the factual and legal issues, nor proportional to the needs of this case. Defendant also objects on grounds that the information sought is not reasonably accessible. Specifically, Defendant objects because: (1) the vast majority of materials Plaintiff requests would result in the production of a large amount of irrelevant, personal health information protected by HIPAA; and (2) recovering a "mirror image" of the backup server(s) or backups of the hard drives connected with Defendant's fax server would be unduly burdensome, as the time and cost involved in recovering the relevant data far outweighs the slight possibility that relevant information would be found. Defendant further objects to this request on grounds that it is vague, as the term "mirror image" is undefined, and its meaning is unintelligible. This request asks Defendant to produce a "mirror image" of any "device used to send facsimile transmissions" but this is not something tangible that Defendant can access and produce.
>
> Moreover, Federal Rule of Civil Procedure 34 does not create a routine right of direct access to a party's electronic information system, and Plaintiff's broad request for production of "mirror images" of Defendant's electronic information systems is beyond the scope of discovery permitted by the Federal Rules.

(Def.'s Resp. Pl.'s First Prod. Req., attached as Exhibit 5, at Nos. 5, 8, 9) (emphasis added). To its responses to Request Nos. 8 and 9, Defendant also stated the following:

> Subject to and without waiving these objections, Defendant states that it has already searched for documents or "templates" for the facsimile at issue in this lawsuit in response to Request to Produce No. 1 in the *Geismann v. American Homepatient* matter, and was unable to locate any responsive documents. Given that Defendant has already searched for, and been unable to locate, the document that this request purports to seek, Plaintiff's request for a "mirror image" of "each hard drive, backup server, or any device used to create, edit, modify, store, or use in any way" the list of intended recipients is unduly cumulative and not

proportional to the needs of this case.

(*Id*., Nos. 8, 9).

Following Defendant's responses to Plaintiff's written discovery, the parties exchanged letters attempting to resolve the discovery issues set forth above (and other discovery issues). (*See* Plaintiff's Nov. 22, 2017 and Dec. 21, 2017 Letters, attached as Exhibits 6 and 7, respectively, and Defendant's Dec. 8, 2017 Letter, attached as Exhibit 8). Thereafter, on January 12, 2018, Defendant served purported Supplemental Responses to Plaintiff's production requests but as to Requests 5, 8, and 9, the "Supplements" were essentially identical to the original responses. (Def.'s Suppl. Resp. Req. Prod., attached as Exhibit 9, at Nos. 5, 8, 9).

Also on September 29, 2017, Plaintiff served its First Set of Interrogatories, including Interrogatory No. 22, which asked: "State the data storage capacity of the fax server hard drive and the brand, model number and serial number of the hard drive in 2013." (Pl.'s First Set Interrogs., attached as Exhibit 10, at No. 22). Defendant asserted several objections and then stated it was without knowledge or information sufficient to answer Interrogatory No. 22. (Def.'s Resp. First Set Interrogs., attached as Exhibit 11, at No. 22). Defendant also "supplemented" its response to Interrogatory No. 22, again asserting the identical answer and adding that "Subject to and without waiving these objections, Defendant states that it is without knowledge or information sufficient to respond to this Interrogatory." (Def.'s Suppl. Resp. Interrogs., attached as Exhibit 12, at No. 22).

D. Defendant rejects Plaintiff's proposed protective order regarding forensic imaging of Defendant's SAN system.

Along with its written discovery requests, Plaintiff also sent Defendant a proposed Agreed Protective Order Regarding Computer Forensic Discovery. (Sept. 29, 2017 email and proposed protective order attached as Exhibit 13). The proposed protective order provided for

forensic imaging of relevant servers by a certified computer examiner, examination of the forensic images by Plaintiff's expert Robert Biggerstaff, compilation of relevant materials on a CD or other electronic media by Biggerstaff for Defendant's initial review, and subsequent production to Plaintiff of the relevant materials. (*See* Ex. 13, Proposed Protective Order, at ¶¶ 1-10). All materials contained in the imaged servers would be deemed confidential pursuant to the Stipulated Protective Order entered by the Court on October 23, 2017. (Stipulated Protective Order, Doc. 27, at ¶ 2). Defendant rejected Plaintiff's proposed Protective Order in its December 8, 2017 letter. (Def.'s Dec. 8, 2017 Ltr. at 5, Ex. 8).

E. Plaintiff's proposed Protective Order Regarding Electronic Discovery ("EPO").

As stated, Plaintiff has attached as Exhibit 1 to this Memorandum its proposed EPO. The proposed EPO provides for the retention of a certified computer examiner ("CPE"), with expertise in the field of electronic discovery, to conduct the acquisition and imaging of Defendant's SAN system *i.e.*, ELECTRONIC DATA, including but not limited to the data contained in the RightFax program, and to preserve its integrity. (EPO, ¶¶ 1, 2, Ex. 1). The CPE (paid for by Plaintiff) will not review or analyze the ELECTRONIC DATA and will not provide the ELECTRONIC DATA to Plaintiff or its counsel. (*Id.*, ¶ 1) The CPE will send the forensic image copy to Biggerstaff and to Defendant's counsel. (*Id.*, ¶ 3).

Biggerstaff will review all relevant ELECTRONIC DATA to the extent practicable for the purposes set forth in the EPO and will not provide the ELECTRONIC DATA to Plaintiff or its counsel. (*Id.* ¶ 3). The purpose of the forensic image of Defendant's SAN system is to preserve and allow examination by Biggerstaff of any ELECTRONIC DATA that exists or may have been deleted that could be relevant to a putative class action lawsuit pending in the United States District Court for the Eastern District of Missouri entitled: *Alan Presswood, D.C., P.C. v.*

American Homepatient, Inc., and docketed as case 4:17-cv-01977-SNLJ (the "Class Action"), regarding: (a) telephone or facsimile numbers to which the Subject Faxes were transmitted, names or addresses associated with those facsimile numbers, the dates the Subject Faxes were transmitted, and whether the transmissions were successful; (b) contents of the Subject Faxes, (c) logs of transmissions or exception reports of the Subject Faxes, (d) the subject matter identified in any pleading, discovery or responses thereto, or testimony in the Class Action, (e) any data or evidence relating to the accuracy or veracity of the contents of the ELECTRONIC DATA or testimony related thereto. (*Id.*, ¶ 5).

Subject to the terms of this EPO, Biggerstaff may conduct appropriate procedures pursuant to the scope and purpose of the creation of the mirror image (via forensic software which preserves each sector of data, including both allocated and unallocated space), and to determine what data was deleted or altered and when and how such deletion or alteration occurred. Biggerstaff shall also examine the contents of the ELECTRONIC DATA for information related to any software or user actions designed to delete or prevent recovery of data, or that could otherwise impact forensic examinations or impact the credibility of information recovered. (*Id.*, ¶ 5).

Within fourteen (14) days after his receipt of the ELECTRONIC DATA, Biggerstaff will analyze the ELECTRONIC DATA and identify those contents he believes fall into the categories specified in Paragraph 5 above. Biggerstaff will prepare a list of the data and/or information in the ELECTRONIC DATA that he believes fall into such categories and copy such summary and such data and/or information on CDs, DVDs, or other suitable electronic media, for submission to Defendant's counsel. (*Id.*, ¶ 6).

Within fourteen (14) days after their receipt of the summary and copies of the data and/or information from Biggerstaff, Defendant's counsel may review the summary and the copies of the data and/or information for objections based on responsiveness, privilege and/or any other grounds prior to any data and/or information being provided to Plaintiff or Plaintiff's counsel. (*Id*., ¶ 7). Upon completion of the 14-day review period, or any such extension thereof obtained by Defendant's counsel, they shall promptly produce all responsive, non-privileged, and otherwise unobjectionable data and/or information identified by Biggerstaff to counsel for Plaintiff. Defendant's counsel shall also provide to Plaintiff's counsel a detailed privilege log identifying all documents or other data submitted to it by Biggerstaff that were not produced to Plaintiff's counsel. (*Id*., ¶ 8). Defendant's counsel shall also provide a copy of the privilege log to Biggerstaff.[3]

Biggerstaff shall not discuss with or disclose to either Plaintiff or Plaintiff's counsel the contents of any data, information, or other materials not produced to Plaintiff's counsel pursuant to Paragraph 8 above, nor will Biggerstaff discuss or disclose any portion of the contents of the SAN system image that he does not identify pursuant to paragraph 6 to any person or entity, including Plaintiff or its counsel, at any time. (*Id*., ¶¶ 9, 10). Biggerstaff shall not disclose any portion of the list of the information identified pursuant to Paragraph 6 above to Plaintiff or its counsel, or discuss same with Plaintiff or his counsel, until Defendant's time for asserting objections has passed. If Defendant asserts objections to all or part of the information identified pursuant to Paragraph 6 above under the procedures of this Order, Biggerstaff shall not disclose such data or any portions thereof to Plaintiff or its counsel unless and until the Court overrules such objections. (*Id.*) Biggerstaff shall not disclose any portion of the information identified

[3] Either party may request a reasonable extension of the foregoing time restrictions. (EPO, ¶¶ 6, 8, Ex. 1)

pursuant to Paragraph 6 above to any person or entity at any time, other than to Plaintiff or his counsel under the terms of this Order. (*Id.*)

Finally, Plaintiff and Biggerstaff agree that they shall return to Defendant through its counsel, or destroy, all copies of documents and data in any format or on any medium whatsoever, provided pursuant to this EPO, and shall destroy all copies of any notes, summaries, compilations or other documents referring to the contents of the aforementioned documents and data, in any format or on any medium whatsoever, within seven (7) days of receiving notice of the conclusion of this litigation. (*Id.*, ¶ 11). Plaintiff and Biggerstaff agree to provide written certification to that effect to Defendant's counsel within 7 days after the destruction. (*Id.*)

Standards for Rule 37 motion to compel

Pursuant to Rule 26(b)(1) of the Federal Rules of Civil Procedure, "[P]arties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case, considering the importance of the issues at state in the litigation, the amount in controversy, the parties relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit. Information within this scope of discovery need not be admissible to be discoverable." Fed. R. Civ. P. 26(b)(1); *Ameriwood Indus., Inc. v. Liberman*, 2006 WL 3825291, at *1 (E.D. Mo., Dec. 27, 2006). Rule 34(a)(1)(A) provides for the production of "any designated documents or electronically stored information—including writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations—stored in any medium from which information can be obtained either directly or, if necessary, after translation by the responding party into reasonably usable form." Fed. R. Civ. P. 34(a)(1)(A).

A party may file a motion to compel discovery under Rule 37(a)(3)(B)(iv) where a party fails to produce documents or fails to respond that inspection will be permitted—or fails to permit inspection—as requested under Rule 34. Fed. R. Civ. P. 37(a)(3)(B)(iv); *Mayberry v. SSM Health Businesses*, 2016 WL 3458164, at *2 (E.D. Mo. June 24, 2016). Upon a showing of relevance by the requesting party, the burden is upon the resisting party to explain why discovery should be limited. *Id*. at *2. In ruling on motions to compel discovery, courts have "consistently adopted a liberal interpretation of the discovery rules" and "look disfavorably upon significant restrictions placed upon the discovery process." *Lanigan v. Babusch*, 2011 WL 5118301, at *1 (N.D. Ill. Oct. 27, 2011) (citation omitted).

Argument

I. Defendant should be ordered to comply with Request Nos. 5, 8, and 9 (and permit the imaging of its SAN), and should be required to answer Interrogatory No. 22

As set forth above, Plaintiff's Request Nos. 5, 8, and 9 request an image of the hard drive, backup server, or any device used to send Exhibit A, attached to the petition, and any other fax advertisements sent by Defendant during class period; in other words, Defendant's SAN storage. (*See* Pl.'s First Req. Prod., Nos. 5, 8, 9, Ex. 4). It is not unusual for a court to enter an order requiring the mirror imaging of the hard drives of any computers that contain documents responsive to an opposing party's request for production of documents. *Balboa Threadworks, Inc. v. Stucky*, 2006 WL 763668, at *3 (D. Kan. Mar. 24, 2006).[4]

In *Ameriwood Indus.*, 2006 WL 3825291, at *1, this Court granted a motion to compel that sought mirror images of all computers used by any defendant (former employees of plaintiff) in a case alleging, *inter alia*, violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030,

[4] A "mirror image" is generally described as a "forensic duplicate, which replicates bit for bit, sector for sector, all allocated and unallocated space, including stack space, on a computer hard drive." *Balboa Threadworks*, 2006 WL 763668, at *3.

and Misappropriation of Trade Secrets, where it was claimed that defendants and their recently formed company improperly used plaintiff's computers and confidential information regarding its ready-to-assemble television stand business. Although the Court noted that courts have been "cautious" in requiring the mirror imaging of computers where the request is extremely broad and the connection between the computers and the claims are "unduly vague or unsubstantiated," the Court further stated that where the defendant used the computer to commit the wrong that is subject to the lawsuit, or where there are "discrepancies or inconsistencies" in the responding party's answers, the hard drive is discoverable. *Ameriwood Indus.*, 2006 WL 3825291, at *4; (emphasis added); *see also Balboa Threadworks*, 2006 WL 763668, at *3 (courts have granted permission to obtain mirror images of computer equipment which may contain electronic data related to the alleged violation).

In fact, courts have repeatedly ordered the imaging of hard drives in TCPA advertising fax cases, whether contested or agreed, each with Biggerstaff as the expert. For example, in *Whiteamire Clinic, P.A., Inc. v. Quill Corp.*, 2013 WL 5348377, at *3 (N.D. Ill. Sept. 24, 1013), a TCPA advertising fax case, plaintiff sought production of an image of the hard drive used to send the faxes at issue. The defendant stored its data using four interconnected proprietary systems and contended that none of the systems contained an image of the fax "as-sent," and that it would have to manually search through the electronic information from several hundred thousand customers to determine who received the fax. Plaintiff disagreed, stating it had an expert (Biggerstaff) who could conduct the search electronically, at plaintiff's expense and pursuant to a protective order. *Id.* at *4. Moreover, defendant could review the material with Biggerstaff before it was provided to plaintiff. *Id.* The court ordered defendant to produce the electronic data, stating:

> [t]he best way to allow plaintiff the ability to see whether these databases can be used to identify which customers received which faxed advertisements is by requiring Quill to produce an image of the hard drives of the four systems and allow plaintiff's expert to review the information under the following protocol: (a) the information will be produced pursuant to a protective order that preserves its confidentiality; (b) efforts to retrieve relevant information will be made in the first instance by plaintiff's expert, Mr. Biggerstaff, along with a defense expert and/or defense counsel if Quill chooses to have one participate; (c) the information that is retrieved will not be available to plaintiff's counsel to review until Quill first has an opportunity to review it for responsiveness to the discovery requests; and (d) plaintiff will bear the cost of Mr. Biggerstaff's work.

Id. at *6; *see also Brodsky v. HumanaDental Insurance Co.*, 2015 WL 13427766, at *3 (N.D. Ill. Feb. 24, 2015) (granting motion to compel image of hard drive in TCPA advertising fax case); *Environmental Progress, Inc. v. Metropolitan Life*, Case No. 12 cv 80907 (S.D. Fla. Dec. 5, 2012 (Doc. 42), at ¶ 3 (Agreed Protective Order Regarding Computer Forensic Discovery, attached hereto as Exhibit 14 (directing defense counsel to "send a forensic image of the Dell Optiplex GX620 direct to Robert Biggerstaff ("Biggerstaff"), Plaintiff's expert"); *Physicians Health, Inc. v. A-S Solutions LLC*, Case No. 12 cv 5105 (N.D. Ill. Oct. 22, 2013) (Doc. 56), at ¶ 3 (Agreed Protective Order Regarding Computer Forensic Discovery, attached hereto as Exhibit 15) (directing certified computer examiner to "send the forensic image copy to Robert Biggerstaff ("Biggerstaff"), Plaintiff's expert"); *Brodsky v. Kaigler & Company*, Case No. 08 CH 44036 (Cir. Ct. Ck. Cy., Ill. June 7, 2011), (Agreed Protective Order Regarding Computer Forensic Discovery, attached hereto as Exhibit 16), at ¶ 4 (directing computer and technology company to "provide the results of the ELECTRONIC DATA recovery to Biggerstaff").

Here, the fax transmission logs are critical evidence both as to class certification and the merits. In *St. Louis Heart Center, Inc. v. Vein Centers* ("*Vein Centers I*"), 2017 WL 492778, at *4 (E.D. Mo. Feb. 2, 2017), a TCPA advertising fax case wherein a class was certified, Judge Perry made clear the importance of fax transmission logs in denying plaintiff's motion for summary judgment, stating "[W]ithout fax logs of successful transmissions or other such

evidence, no potential class member can prove they were "sent" a junk fax, as required by the class definition[,]"and that "[U]nless Heart Center has other evidence proving that notified class members were successfully sent a junk fax, this case appears ripe for summary judgment for Vein Centers." In a later opinion, Judge Perry decertified the class based on the same rationale – that plaintiff could not demonstrate which fax numbers were successfully sent a junk fax in the absence of fax transmission logs "or other such evidence." *St. Louis Heart Center, Inc. v. Vein Centers* ("*Vein Centers II*"), 2017 WL 492778, at *5 (E.D. Mo. Feb. 2, 2017). *Vein Centers II* is currently on appeal in the Eight Circuit, No. 17-3239, and is set for oral argument on April 11, 2018.

In addition, the connection between the SAN system and the TCPA claims at issue are not "unduly vague or unsubstantiated" but are direct – the transmission logs and other evidence of the faxing at issue should be located in the SAN system, as explained by Biggerstaff, underscoring that Defendant should be compelled to produce the requested forensic image. *Ameriwood Indus.*, 2006 WL 3825291, at *4; *Balboa Threadworks*, 2006 WL 763668, at *3. Even Defendant concedes Biggerstaff may locate the fax transmission logs – "the slight possibility that relevant information would be found." (*See* Def.'s Resp. Pl.'s First Prod. Req., at Nos. 5, 8, 9, Ex. 5). Defendant's "slight possibility" assertion was couched in terms of "undue burden," but it is Plaintiff who will pay for the forensic imaging and Biggerstaff's efforts. Defendant's objection that the requested imaging "seeks information not relevant to the factual and legal issues, nor proportional to the needs of this case" is unsustainable if not frivolous, particularly in light of Judge Perry's opinions in *Vein Centers I* and *Vein Centers II*.

Related to the imaging of the SAN, Defendant should be required to answer Interrogatory No. 22 and provide the data storage capacity of the fax server hard drive and the brand, model

number and serial number of the hard drive in 2013, *i.e.*, the specifications of the SAN system. This information is necessary to enable the CPE to image the SAN system. Without said information, the CPE will not know the equipment necessary to accomplish the forensic image.

Finally, Plaintiff anticipates Defendant will argue that HIPAA regulations weigh against the requested imaging. On the contrary, HIPAA regulations, at 45 C.F.R. § 164.512(e)(1), expressly permit protected health information to be revealed in response to a discovery request, if the parties agree to a protective order and have presented it to the court or have asked the court for a protective order. *U.S. ex rel. Camillo v. Ancilla Systems, Inc.*, 233 F.R.D. 520, 522 (S.D. Ill. 2005) (citing 45 C.F.R. 164.512(e)(1)); *see also Bayne v. Provost*, 359 F. Supp. 2d 234, 237 (N.D.N.Y. 2005) (HIPAA and its implementing regulations "unequivocally" permit health care providers and other covered entities to disclose protected health information without patient consent in judicial proceedings).

A "qualified protective order" means a protective order that "prohibits the parties from using or disclosing the protected health information for any purpose other than the litigation or proceeding for which such information was requested" and "requires the return to the covered entity or destruction of the protected health information (including all copies made) at the end of the litigation or proceeding." 45 C.F.R. 164.512(e)(1)(v)(A-B); *United States. v. Bek*, 493 F.3d 790, 802 (7th Cir. 2007) (finding it appropriate to enter a protective order pursuant to HIPAA). In short, The proposed EPO is a "qualified protective order" under HIPAA.

Conclusion

WHEREFORE, Plaintiff requests that the Court enter an Order requiring that Defendant answer Interrogatory No. 22, and that the Court entered Plaintiff's proposed Protective Order Regarding Electronic Discovery, and other relief set forth in Plaintiff's Motion.

Respectfully submitted,

/s/ Max G. Margulis
Max G. Margulis
Margulis Law Group
28 Old Belle Monte Rd.
Chesterfield, MO 63017
Telephone: 636-536-7022 – Residential
Fax: 636-536-6652 – Residential
Email: maxmargulis@margulislaw.com

Brian J. Wanca, IL # 3126474IL
Anderson + Wanca
3701 Algonquin Rd., Suite 500
Rolling Meadows, IL 60008
Telephone: 847-368-1500
Fax: 847-368-1501
Email: bwanca@andersonwanca.com
Attorneys for Plaintiff Alan Presswood, D.C., P.C.

CERTIFICATE OF SERVICE

I hereby certify that on the 20th day of March, 2018, I submitted the foregoing via this Court's CM/ES system, which served notice of the filing on the Attorneys for Defendant, John C. Ochoa (6302680IL), Molly Arranz (6281122IL), SmithAmundsen LLC, 150 North Michigan Avenue, Suite 3300, Chicago, IL 60601; P: 312-894-3200, F: 312-997-1843, Email: JOChoa@salawus.com, and marranz@salawus.com and a courtesy copy was also served by email.

/s/ Max G. Margulis